(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 915 590 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
29.09.2004 Bulletin 2004/40

(51) Int Cl.[7]: **H04L 9/32**

(21) Application number: **98309195.0**

(22) Date of filing: **10.11.1998**

(54) **Method and system for secure lightweight transactions in wireless data networks**

Verfahren und Vorrichtung zur Leichtgewichtstransaktion in drahtlosen Datennetzwerken

Procédé et dispositif pour une transaction sécurisée et légère dans des réseaux de données sans fil

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI NL PT SE

(30) Priority: **10.11.1997 US 966988**

(43) Date of publication of application:
12.05.1999 Bulletin 1999/19

(73) Proprietor: **Phone.Com Inc.**
Redwood City, CA 94063 (US)

(72) Inventors:
- **Liao, Hanging**
  San Ramo, CA 94583 (US)
- **Boyle, Stephen S.**
  Fremont, CA 94539 (US)
- **King, Peter F.**
  Half Moon Bay, CA 94019 (US)
- **Schwarz, Bruce V.**
  San Mateo, CA 94402 (US)

(74) Representative: **Suèr, Steven Johannes et al**
Ablett & Stebbing,
Caparo House,
101-103 Baker Street
London W1M 1FD (GB)

(56) References cited:
US-A- 5 668 875

- **NEEDHAM R M ET AL: "Using encryption for authentication in large networks of computers" COMMUNICATIONS OF THE ACM, DEC. 1978, USA, vol. 21, no. 12, pages 993-999, XP002163714 ISSN: 0001-0782**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 915 590 B1

Description

[0001] The invention relates to wireless data communications, and more particularly relates to secure lightweight transactions between mobile devices and landline servers over wireless data networks; wherein the mobile devices have very limited computing power, memory and graphical display capability.

[0002] A fast-growing trend on the Internet is electronic commerce. The electronic commerce is an integrative concept designed to draw together a wide range of business support services, trading support systems for commodities, products, customized products and custom-built goods and services; ordering and logistic support systems; settlement support systems; and management information and statistical reporting systems, all via the Internet. It is well known, however, that the Internet is a wide open, public and international network of interconnected computers and electronic devices around the world. Anyone who has access to a computer in the network can intercept signals carrying proprietary information traveling along the network. To transact business over the open network, companies or individuals must have an efficient, reliable and secured manner to conduct private communications therebetween. Security thus becomes a primary concern over the open Internet and there have been many efforts in progress aimed at protecting the proprietary information travelling in the Internet. One of the efforts is to use cryptographic techniques to secure a private communication between two parties. The cryptographic techniques provide a way to transmit information across untrusted communication channel without disclosing the contents of the information to anyone accessing the communication channel.

[0003] US Patent No. 5,671,279 to Taher Elgamal discloses a courier electronic payment system for conducting the electronic commerce using a secure courier system. The system governs the relationship between a customer, merchant, and acquirer gateway to perform credit card purchases over the open network by using a secure connection to simplify the problem of Internet-based financial transactions. Visa International Service Association. in collaboration with Microsoft Corporation, provides a secured transaction technology using digital signature to authenticate a credit card and merchant decal, referring to http://www.visa.com for detail. The technologies developed by RSA Data Security, Inc. are the global de facto standard for public key encryption and digital signature and may be part of existing and proposed standards for the Internet as well as business and financial networks around the world. More information about the Internet security can be found at http://www.rsa.com.

[0004] The above and other ongoing efforts are all primarily targeted at the Internet that is a plurality of landline or wired networks. To use the Internet, one has to have a physical access to a computer wired into the network. To provide the mobility of the network, wireless data networks were introduced, as such the landline networks become an integral part of the wireless data networks. With the wireless data networks. people, as they travel or move about, are able to perform, through wireless computing devices or handheld communication devices, exactly the same tasks as they could do with computers in the landline networks. Similar to the Internet, however, the nature of the wireless communications provides an opportunity for intrusion since the mobile data is sent through the air. Anyone who has an appropriate receiver with a designed antenna can intercept signals being communicated between a wireless computing device and a landline base-station or network. Privacy, authentication. authorization, and integrity are thus deemed the important elements in wireless data network. Therefore additional efforts have been started to ensure that the proprietary information is sent via wireless networks that must be restricted only to those with a need to know.

[0005] Many networks employ encryption and other security measures to protect mobile data from access by unauthorized third party. Certain technologies and access methods contribute to network security. Spread spectrum technology, for example, is inherently secure, but it only provides a link level security. There is no guarantee that a mobile device has a secure communication to a landline device through a complete wireless network that generally comprises an aimet, the Internet and a gateway therebetween. US Patent No. 5.604.806 to Hassan, et al, discloses an apparatus and method for secure radio communication by using key sequences derived from the short-term reciprocity and radio spatial decorrelation of phase of the radio channel. US Patent 5.371.794 to DIFFIE et al. shows another method and apparatus for providing a secure communication between a mobile wireless data processing device and a base data processing device. The mobile device sends the base device a digitally signed mutually trusted certificate according to a public encryption key and the base device sends a modified version to the mobile device upon successfully recovering the certificate. If the mobile device recovers the modified version, both devices enter a secure data communication. The disclosed system by DIFFIE may work well with mobile devices that have competitive computing resources to satisfy the public-key-based encryption speed. Nevertheless the connection time in an aimet is expensively measured and many mobile devices such as mobile phones have a small fraction of the computing resources provided in a typical desktop or portable computer. The computing power in a typical cellular phone is less than one percent of what is in a regular desktop computer. the memory capacity thereof is generally less than 250 kilobytes and the LCD display is perhaps four lines high by twelve or twenty characters, the graphics capabilities thereof are very limited or nearly nonexistent. There has been thus a great need for a generic solution that provides a se-

cure communication with competitive performance between mobile devices of limited computing resources and landline devices through an open network.

[0006] Further many current networks operate based on Hypertext Transfer Protocol (HTTP) that is built on the Transmission Control Protocol/Internet Protocol (TCP/IP). But the TCP protocol requires considerable computing power and network bandwidth resources. A single connection, for example, may require an exchange of more than ten packets between a sender and a receiver in the Internet. Therefore there has been further a need for a generic method and system that provide a secure communication between mobile devices and landline devices using fewer number of packets so as to increase transmission efficiency in mobile devices of limited computing resources.

[0007] According to one aspect of the present invention there is provided a method for establishing an authenticated and secure communication session for transactions between a client and a server over a wireless data network, said client being remotely located with respect to said server, said method comprising:-

sending a session-request signal from said client over said wireless data network to said server, said session-request signal including a client message, which is encrypted according to a shared secret encrypt key previously residing on both the client and the server;

conducting a first step of a client authentication at the server by checking for the successful decryption of the encrypted client message according to said shared secret encrypt key;

generating at the server a session key for said session, a first derivative of the decrypted client message, and a server message if the first step of the client authentication is successful;

sending a session-reply signal from said server to said client over said wireless data network, said session-reply signal including said session key, said first derivative of the decrypted client message, and said server message, which are encrypted according to said shared secret encrypt key;

conducting a first step of a server authentication at said client by checking for the successful decryption of the encrypted session-reply signal according to said shared secret encrypt key, and retrieving said first derivative of the decrypted client message and said server message;

conducting a second step of the server authentication at said client by validating the first derivative of the client message with the client message included in the session-request signal;

generating at the client a first derivative of the decrypted server message if the server authentication is successful;

sending a session-complete signal (SC, 148) from said client to said server over said wireless data network, said session-complete signal including said first derivative of the decrypted server message, said first derivative being encrypted according to said shared secret encrypt key;

conducting a second step of the client authentication at said server by validating the first derivative of the decrypted server message with the server message included in the session-reply signal; and

establishing an authenticated and secure communication session if the second step of the client authentication is successful.

[0008] Upon the establishment of the secure communication between the client and the server, either the client or the server may initiate a transaction therebetween. To ensure the transaction between a valid session, the transaction is encrypted by a mutually accepted cipher according to the session key and identified by a session ID embedded therein. The mutually accepted cipher can be obtained by the server through a cipher negotiation with the client and the transaction ID in the transaction is always examined in the server before the server responds to the client with a service reply. Upon receiving the service reply from the server, the client can proceed the transaction with the server.

[0009] Preferably, said session-request signal further includes a modified version of said client message, encrypted according to said shared secret encrypt key; wherein said modified version has an operational relationship with said client message.

[0010] In one embodiment, said first derivative of the client message has a mathematical relationship with said client message.

[0011] Conveniently, said client message comprises a client nonce.

[0012] In another embodiment, said first derivative of the server message has a mathematical relationship with said server message.

[0013] Preferably, said server message comprises a server nonce.

[0014] Conveniently, said session-complete signal is piggybacked by a transaction request from said client.

[0015] In one embodiment, said transaction request is encrypted according to said session key included in the session-reply signal.

[0016] In a preferred embodiment, said session-request signal further includes a device identifier associated with the client, and wherein the server determines said shared secret encrypt key based on the device identifier.

[0017] It is preferred that the session-request signal includes a client cipher indicating what encryption the client currently uses.

[0018] It will be apparent that the method can further comprise the step of the server negotiating a mutually accepted cipher with the client for the session.

[0019] According to another aspect of the present invention there is provided an apparatus for establishing

an authenticated and secure communication session for transactions with a server over a wireless data network, said server being remotely located with respect to said apparatus, said apparatus comprising:-

a display screen;
memory for storing code for a client module;
a processor coupled to said memory, said processor executing said code in said memory to cause said client module:-

to send a session-request signal over said wireless data network to said server, said session-request signal including a client message, which is encrypted according to a shared secret encrypt key previously residing on both the apparatus and the server;
to conduct a first step of a server authentication by checking for the successful decryption of a session-reply signal, received from said server in response to said session-request signal, encrypted according to said shared secret encrypt key, and retrieving a first derivative of said client message and a server message;
to conduct a second step of the server authentication at said client by validating the decrypted first derivative of the client message with the client message included in the session-request signal;
to generate a first derivative of the decrypted server message if the server authentication is successful; and
to send a session-complete signal to said server over said wireless data network, said session-complete signal including said first derivative of the decrypted server message, said first derivative being encrypted according to said shared secret encrypt key.

[0020] Preferably, said session-request signal further includes a modified version of said client message, encrypted according to said shared secret encrypt key; wherein said modified version has an operational relationship with said client message.

[0021] In one embodiment, said first derivative of the client message has a mathematical relationship with said client message.

[0022] Conveniently, said client message comprises a client nonce.

[0023] In another preferred embodiment, said processor causes said client module to piggyback a transaction request on said session-complete signal.

[0024] In one embodiment, said processor causes said client module to encrypt said transaction request according to said session key included in the session-reply signal.

[0025] In another embodiment, said session-request signal further includes an apparatus identifier so that the server can determine said shared secret encrypt key based on the apparatus identifier.

[0026] Conveniently, the session-request signal includes a client cipher indicating what encryption the apparatus currently uses.

[0027] Accordingly, an important object of the present invention is to provide a generic solution for secure lightweight transaction in wireless data networks. Other objects, together with the forgoing are attained in the exercise of the invention in the following description and resulting in the embodiment illustrated in the accompanying drawings.

[0028] These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description. appended claims, and accompanying drawings where:

Figure 1 shows a schematic representation of a mobile data network in which the present invention may be practiced;
Figure 2 depicts a block diagram of a typical GSM digital cellular phone used in the embodiment of the disclosed invention;
Figure 3 illustrates the process of mutual authentication between a client and a sever;
Figure 4.a and Figure 4.b depict a data flowchart representing the session creation process in the client and the server, respectively, of Figure 3 in one embodiment of the present invention;
Figure 5 shows a schematic diagram of a service transaction;
Figure 6 shows a schematic diagram of a notification transaction; and
Figure 7 shows a schematic diagram of a post transaction.

[0029] The detailed description of the present invention in the following are presented largely in data flowing representation that resemble the operations of data processing devices coupled to networks. These process descriptions and representations are the means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. The present invention is a method and system for secure data communications. The method along with the system or architecture to be described in detail below is a self-consistent sequence of steps leading to a desired result. These steps or processes are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities may take the form of electrical signals capable of being stored, transferred, combined, compared, displayed and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, operations, messages, terms, numbers, or the like. It should be borne in mind that all of these similar terms are to be associated with the appropriate physical quan-

tities and are merely convenient labels applied to these quantities.

[0030] Referring now to the drawings, in which like numerals refer to like parts throughout the several views. Figure 1 shows a schematic representation of a wireless data network 100 in which the present invention may be practiced. The data network 100 comprises an aimet 102 and the landline network 104, each acting as a communication medium for data transmission therethrough. The landline network 104 may be the Internet, the Intranet or other private networks. For simplicity, the landline network 104 will be herein simply referred to as the Internet, literally meaning either the Internet or the Intranet or other private network. Further the airnet 102, meaning unwired network in which data transmission is via the air, is sometimes referred to as a carrier network because each aimet is controlled and operated by a carrier, for example AT&T and GTE. each having its own communication scheme. such as CDPD, CDMA, GSM and TDMA. Referenced by 106 is a mobile data device, but resembling a mobile phone, in communication with the aimet 102 via an antenna 108. It is generally understood that the aimet 102 communicates simultaneously with a plurality of mobile computing devices of which a mobile phone 106 is shown in the figure. Similarly connected to the Internet 104 are a plurality of desktop PCs 110 and a plurality of web servers 112. though only one representative respectively shown in the figure. The PC 110. as shown in the figure, may be a personal computer SPL 300 from NEC Technologies Inc. and runs a web browser via the Internet 104 to access information stored in the web server 112 that may be a workstation from SUN Microsystems Inc. It is understood to those skilled in the art that the PC 110 can store accessible information so as to become a web server as well. Between the Internet 104 and the aimet 102 there is a link server 114 performing data communication between the Internet 104 and the aimet 102. The link server 114, also referred to as link proxy or gateway, may be a workstation or a personal computer and performs a protocol mapping from one communication protocol to another, thereby a mobile device 106 can be in communication with any one of the web servers 112 or the PCs 110, respectively.

[0031] The communication protocol in the Internet 104 is HTTP that runs on TCP and controls the connection of an HTML Web browser to a Web server and the exchange of information therebetween. An extended version thereof, called HTTPS, provides encrypted authentication and session transmission between a client and a server. The communication protocol between the mobile device 106 and the link server 114 via the aimet 102 is Handheld Device Transport Protocol (HDTP), or Secure Uplink Gateway Protocol (SUGP), which preferably runs on User Datagram Protocol (UDP) and controls the connection of a HDML Web browser to a link server, where HDML stands for HandHeld Markup Language. The specification thereof and the HDTP specification are provided at http://www.w3.org or http://www.uplanet.com that are incorporated herein by reference. Further a reference specification entitled "Magellan SUGP Protocol" is incorporated herein by reference. The HDTP is a session-level protocol that resembles the HTTP but without incurring the overhead thereof and is highly optimized for use in mobile devices that have significantly less computing power and memory. Further it is understood to those skilled in the art that the UDP does not require a connection to be established between a client and a server before information can be exchanged, which eliminates the need of exchanging a large number of packets during a session creation. Exchanging a very small number of packets during a transaction is one of the desirous features for a mobile device with very limited computing power and memory to effectively interact with a landline device.

[0032] According to one preferred embodiment, the present invention may be practiced with a cellular phone, a typical example of the mobile device 106, that has very limited computing power and memory. The cellular phone 106 is used as a client in communication to a landline device that is often referred to as a server providing accessible information therein to other devices. Figure 2 shows a block diagram of a typical GSM digital cellular phone 120. Each of the hardware components in the cellular phone 120 is known to those skilled in the art and so the hardware components are not to be described in detail herein. Although the user interface of the phone 120 is not shown in the figure, the mobile device 118, resembling a cellular phone, in Figure 1 may be referenced thereto, in which referenced by 116 is a LCD screen and 118 is a key button pad, respectively. Through the screen 116 and the keypad 118 controlled by a user of the phone, the phone can be interactively communicated with a server through the aimet, link server and the Internet. According to one embodiment of the present invention, complied and linked processes of the present invention are stored in ROM 122 as a client module 124 and support module 126. Upon activation of a predetermined key sequence utilizing the keypad 118. a physical layer processor or microcontroller 118, initiates a session communication to the server using the module 124 in the ROM 122.

[0033] To establish a secured communication between a client and a server, an authentication process must be conducted first to ensure that only interested parties are actually in the communication therebetween. The process is complete through two rounds of independent authentication. one being the client authenticated by the server. referred to as client authentication, and the other being the server authenticated by the client, referred to as server authentication. Further each authentication is completed in two separate steps for high grade of security, which will be described in detail below. The success of the mutual authentication processes provision an evidence that the two communicating parties possesses a valid shared secret encrypt key

through a mutual decryption and a challenge/response mechanism. The mutual decryption mechanism comprises the steps of mutually recovering encrypted messages from two involved communicating parties. The challenge/response mechanism, referred to as nonce verification, verifies a predetermined relationship between a sent nonce and a received derivative thereof.

[0034] In one preferred embodiment of the present invention, the authentication process is conducted with three message exchanges; a Session Request (SR), a Session reply (SP), and a Session Completion (SC). Figure 3 illustrates a schematic representation of the authentication process. The client 140, representing a mobile device, to conduct a transaction with the server 142, representing a landline server or PC. initiates a SR 144 to be sent to the server 142 by first creating a client proto-session. A client proto-session is a session data structure that gets initialized when a session creation starts. The initialized SR 144 comprises the following information:

sessionID - an identifier identifying all requests from the client to the server; In the case of requesting a session creation. sessionID is always assigned to 0;

cipher - a two-byte number representing the choice of the encryption the client is currently using as there are a number of encryption schemes available in a communication protocol;

version - a one byte number representing the HDTP protocol version in use. used to determine the underlying format of the communication protocol such as PDU;

type either a fixed five-byte number representing what device the client is, e.g. 2PCSI means the client is a PCSI phone version 2.

deviceID - a variable up to 255-byte, representing the device identifier or the client identifier comprising, a phone number of the devcie or an IP address and a port number, e.g. 204,163,165,132:01905 ;

header - up to 32767 bytes, comprising token/value pairs that apply to an entire session and may be automatically applied to subsequent service requests or session specific parameters, therefor the header is generally cached in the server till the current session completes; and

C-nonce - a client nonce represented with a non-repeatable number, usually 2 bytes, used for the client to conduct a following server authentication.

C-nonceModified - a modified version of the client nonce, used for the server to conduct a nonce verification in the following client authentication.

[0035] Further the cipher in the SR 144 includes an identifier to an encryption algorithm and associated parameters thereof. To be more specific. the first byte in the cipher represents an identifier to a combination of the encryption algorithm, the key size (e.g. 128-bit for US or 40-bit for foreign countries) and content of a security attachment thereto and the second byte in the cipher indicates the additional parameters related to the first byte. For example, value 1 in the first byte indicates that the encryption algorithm is block cipher RC5, the key size thereof is 128 bit. a two byte check-sum therein is used as the MAC (Message Authentication Code), no IV (Initialization Vector for block ciphers) therefor is transmitted over the network, and padding bytes are added if necessary. The block cipher algorithm RC5 is part of the RSA's BSAFE product. It can be further appreciated that the identifier in the cipher may be assigned to a unique value to identify a non-secure session if so desired. The C-nonce is a non-repeatable number initially and randomly generated in the client and the modified version thereof. C-nonceModified. is generated from the C-nonce through a operational relationship; for example the Exclusive-OR relationship or expressed as follows:

C-nonceModified = 2-byte-number $\oplus$ C-nonce. It can be appreciated by those who are skilled in the art that there are many ways to get the C-nonceModified from a C-nonce, the Exclusive-OR is one of the operational relationships used in one embodiment of the present invention. Both C-nonce and C-nonceModified are encrypted using the shared secret encrypt key between the client 240 and the server 142. The purpose of the C-nonceModified is to provide the server that receives the SR with means for ensuring that C-nonce is correctly decrypted and validated by examining the C-nonce and its relationship with the C-nonceModified. Both should not be altered after a successful decryption of the C-nonce and the C-nonceModified. In other words, a SR message or signal may be expressed as follows:

SR = {session ID, cipher, version, type, device ID, header. Encry[nonce. nonceModified]};

where Encry[ ] means that the parameters or contents in the bracket are encrypted accordingly. When the SR is sent by the client to the server to request a session creation, both C-nonce, C-nonceModified are encrypted according to the cipher the client is using at the time the SR is sent out.

[0036] Upon receiving the SR from the client 140, the server 142 creates a server proto session for the client 140 with a session identifier, referred to as session ID, to identify the session context for the session just created in the server 142. A server proto-session is a session entry marked as a proto status in a session table. which indicates that the session is not authenticated and is not able to conduct any transactions with the client. It is understood to those skilled in the art that the proto-session can be kept in the RAM of the server. If a proto-

session already exists for that client. it is re-used. The information in the received SR is saved in the server proto-session. If the server 142 is satisfied with the fact that the client is known, namely Encry[C-nonce, C-nonce-Modified] in the received SR are successfully decrypted with the shared secret encrypt key, the step one in the client authentication is successful and a corresponding session key is generated and stored with the server proto session entry. It may be noted herein that many encryption schemes used in this invention, such as RC5, have a procedure that adds and validates the Message Authentication Code such as the check-sum. to assure that the encrypted message is correctly decrypted, the procedure, every time the decryption takes place, is used herein to examine the transaction integrity, namely to assure the received messages or signals are unaltered in the cause of data transmission. If the step one client authentication is not successful, namely Encry[C-nonce, C-nonceModified] in the received SR are not fully decrypted or supported, the proto session is aborted and removed from the proto session table, resulting in a failed session creation. What the support means herein is the cipher proposed or used by the client is also used by the server, for example the client uses the RC5 encryption to encrypt Encry[C-nonce. C-nonceModified]. to decrypt Encry[C-nonce. C-nonceModified], the server must be equipped with the same RC5 encryption capability therein. If Encry[C-nonce. C-nonceModified] can not be successfully decrypted due to other reasons such as transmission errors. the client must reinitiate a new session request to the server in order to establish a secure communication with the server. To challenge a step two server authentication subsequently at the client side, a derivative of the client nonce or C-nonce, is generated therefor. In one embodiment of the present invention, the derivative is created by adding a constant to the client nonce, for example derivative = C-nonce + 1. The purpose of the derivative is to provide the client with means for reassuring that the C-nonce is correctly decrypted by the server and the server is the authenticated one in communication with.

[0037] Right after the successful step one client authentication. the server 142 responds to the client with a Session rePly (SP) 146 to begin a second round authentication: server authentication. The SP 146 comprises the following information:

C-SID - a one byte number indicates the sessionID originally assigned in the client, to be more specific C-SID = 0 indicates a clear text client session. C-SID = 1 indicates a shared secret key encrypted session, and C-SID = 2 indicates a session key encrypted session. In the context of the current description, C-SID = 1.

sessionID - a four-byte number representing an identification and parameters, such as a session encrypt key, of the session created by the server for the client;

key - a session key to be used with a mutually acceptable encryption, and to be used for encryption and decryption in all transactions in the session;

derivative - a number derived from the C-nonce for the client to perform the subsequent server authentication;

S-nonce - a non-repeatable number, used for the server to conduct a following step-two client authentication; it should be noted that S-nonce is generated by the server and generally different from the C-nonce by the client; and

cipher - a two-byte number representing the choice of the encryption the server proposes after the client proposed cipher is received. it may or may not be the same as the one used in the client, to be more specific, the cipher is the same as the one proposed by the client when the server supports the client proposed cipher, otherwise the cipher is the one currently used in the server.

[0038] In other words, the SP can be expressed as follows:

SP={C-SID. Encry[sessionID, key, S-nonce, derivative, cipher]};

[0039] When the client 140 receives the SP 146 from the server 142, it performs the step one server authentication, which is considered successful if Encry[sessionID, key, S-nonce, derivative. cipher] in the received SP 146 is decrypted successfully with the shared encrypt key. If the step one server authentication fails, the client 140 discards the SP 146 and a new session creation may be started over again. Upon the success of the step one server authentication, the client 140 proceeds with the step two server authentication; namely the predetermined relationship between the C-nonce and the derivative thereof should be hold for a successful step-two server authentication:

C-nonce = derivative -1

[0040] If the C-nonce derived from the SP 146 is the same as the C-nonce originally generated by the client, the step two server authentication is successful, hence the server 142 is considered authenticated, trusted from the viewpoint of the client, and the SP 146 is accepted as a valid message, which means that the client 140 then uses the session key and other information in the SP 146 for the session being created. Only with both successful steps of the server authentication, the client 140 marks the session as committed, which means that transactions can be conducted subsequently in the session, again only from the viewpoint of the client 140. If the predetermined relationship between the client nonce and the derivative thereof does not hold, the step two server authentication fails and the received SP 146

is discarded. The client 140 may abort the session creation process if no further SP's are received and pass both steps of the server authentication during the time period allowed for a session creation. To provide the server with means for reassuring the client authentication by itself through the client, a derivative of the S-nonce, similar to the derivative of the C-nonce, is generated.

[0041] The client 140 then sends the server 142 a SC 148 to complete the session creation process. The SC 148 comprises the following information:

SC= {Encry[derivative]};

where the derivative is the client's response to the server nonce challenge, namely the result of the verification, the derivative is used by the server 142 for step two client authentication. Further it is noted that the SC 148 is an encrypted message, meaning that the client encrypts the information in the SC 148 according to either its own cipher or the server proposed cipher. Generally the client 140 encrypts the information in the SC 148 according to the server proposed cipher if it accepts the server proposed cipher, otherwise, it encrypts the SC according to its own cipher.

[0042] It must be noted in one embodiment of the present invention that the SC unlike the SR 144 and SP 146, is piggybacked by a following transaction request to increase data transmission efficient. The data piggybacking means that independent data units may be logically grouped together in one physical data unit to be transmitted to a receiver that recovers all the independent data units upon the receipt of the physical data unit as if all the independent data units were sent, independently and respectively, in separate physical data units.

[0043] Upon receiving of Session Complete or SC 148, the server 142 tests if the client 140 uses its own proposed cipher or the server proposed cipher by decrypting the SC twice using the two ciphers if necessary. If the server 142 decrypts the encrypted message in the SC 148 and verifies the relationship thereof with the S-nonce, the step two client authentication is succeeded. Subsequently the server 142 promotes the server proto session to the active session and the session creation process is completed; otherwise, the proto session is removed and the session creation is aborted.

[0044] Referring now to Figure 4.a and Figure 4.b, there are shown two data flowcharts 180 and 181 representing a session creation process in the client and the server, respectively, in one embodiment of the present invention. There are generally three types of transactions that are conducted between a mobile device and a landline server; service transaction, notification transaction, and post transaction. Both service and post transactions are initiated by the mobile device that is considered as a client herein and the notification transaction is initiated by the landline server that is considered a server herein. All transactions must be conducted in the context of a valid and established session. If there is no session or valid session, a session must be created before any transaction can start. For the sake of simplicity, it is assumed that the transaction is initiated at the client side at 182. As described above, for a transaction to take place in a secure communication, a session between a client and a server must be established first. Therefore at 184, the existence of a valid session is examined. If a valid session is in place, the transaction can proceed at 186. If there is no established session, for example, a mobile device is just powered on for the first time or a previous session is beyond a time limit, for example 8 hours, a session request must be initiated and sent to the server at 188. The client is then in a mode of waiting for a reply from the server, constantly looking up for the reply at 190 and 192. If there is no reply from the server, the client may initiate another session request if a fixed time period lapses at 194 or errors occur to have to abort the initiated session request at 196 and 198. The errors occur when the client is out of a service area covered by an airnet that communicates with the server or simply either the client or the server malfunctions at 199.

[0045] Meanwhile the session request is received by the server at 216. A proto session is created at 222 per the session request from the client if the session request is not a duplicated one. It is very common that a session request may be retransmitted or re-requested by the client due to some unexpected error conditions in the wireless data network so that duplicated requests may be received. The server, however, uses a tag. which is generated from the encrypted message in the session request first received and is unique for each session request from a particular client, to prevent creating multiple proto sessions from the duplicated session requests. Some of the information in the session request, such as protocol version and device ID are verified at 224. If the verified information is not supported, there might be device error at 226, which results in the removal of the proto session just created. If the verifying process at 224 succeeds, the server proceeds a decryption process, according to a shared secret encrypt key as described above, to decrypt the C-nonce and C-nonceModified at 230. If the operational relationship between the C-nonce and C-nonceModified holds at the server side, the step one client authentication completes. CIP at 203 in Figure 4.a and 234 and 236 of figure 4.b stands for crypto ignition process which is a process to equip a client with a updated encrypt information, for example, to update the share secret key. As the CIP is an added process and not a key element in the present invention, and no detail description thereof is provided therefore. With the successful step one client authentication, the server at 238 sends a session reply to the client.

[0046] When a server is reached and successfully processes the session request from the client, namely the step one client authentication as described above, a session reply is sent by the server to the client to start server authentication at the client side. Upon receiving the session reply from the server being connected, the

client examines the reply signal at 200 and 201 and the session reply should be in a recognized format, such as uncorrupted essential information therein. If the received session reply is not recognized or supported, the client discards the received session reply at 202 and continues to wait for a valid session reply. otherwise problems with devices may be claimed in step 199. Upon receiving the session reply from the server, the client proceeds two steps of the server authentication at 204, which has been described above in detail. Logically the session is discarded at 202 if the server authentication fails, namely the client fails to decrypt and verify the encrypted S-nonce and to validate the derivative of the C-nonce generated by the server. When the server authentication passes, the client chooses either its own cipher or the server proposed cipher obtained from the session reply from the server at 208 and 210 and further the client retrieves the session key therefrom and sends a session complete signal to the server to complete the session creation at 212 and 214.

[0047] Meanwhile the server expects a session complete signal from the client it just sends the session reply to at 238. For security purpose, the server drops the proto session at 242 if the time waiting for the session complete signal goes beyond a threshold 240. Upon receiving the session complete signal at 244, the server proceeds the step two client authentication at 246 and 248 by decrypting the encrypted derivative of the S-nonce and verifying the relationship thereof with the original S-nonce. If the decryption of the derivation or the verification with the S-nonce fails, the session creation fails, hence the removal of the proto session. If the step two client authentication succeeds, that means the step one client authentication and the step one and two server authentication have all completed, the session is successfully created by promoting the proto session to the regular session at 250, thereby the transaction originally initiated by the client at 182 of Figure 4.a can proceed therefrom.

[0048] To perform transactions in an authentic and secure session, each transaction must be assigned to a transaction ID. In one embodiment of the invention, a new transaction must have a new transaction ID and has to be in a trans-sequence, namely the transaction ID must be greater than any other completed and pending transaction IDs and less than 255 at the time the new transaction is started in the session, for example, transaction ID = 12 for a current transaction, the next transaction ID from the client must be 13 or greater in order for the transaction to be accepted by the server. The constant 255 is the maximum number of transactions that can be performed in a valid session. If a transaction ID is smaller than what the session expects, the transaction is discarded without notice. If the transaction ID is greater than 255, a new session is automatically created to accommodate the corresponding transaction. All the data units related to transactions are encrypted with the session key created in the session creation process and the cipher used therein is either the client proposed cipher or the server proposed cipher.

[0049] Referring to Figure 5, there is shown a schematic diagram of a service transaction. The mobile client 140 initiates a Service Request (tSR) 152 to the server 142. A service transaction is typically involved in interaction with a service provider identified by a universal Resource Locator URL in a landline server, therefore the information in a tSR comprising URL and optional header that provides additional session information. Upon receiving the tSR 152, the server 142 processes the received tSR 152 to examine the sessionID and transaction ID therein. If the transaction ID is less than what it expects, the tSR 152 is discarded. In addition, the tSR 152 is discarded if the transaction ID in the received tSR 152 is greater that 255. As described above, for security reason, a maximum of 256 transactions is allowed in a session. If more than the allowed number of transaction occurs in one established session, a new session will be automatically initiated with the transaction ID being started from 0. Upon the successful examination of the service request tSR 152, the server 142 responds with a Service Reply (tSP) 154 that comprises a result in the form of digest of the URL service request and an optional header. Upon receiving the tSP 154 from the server 142, the client 140 sends the server 142 an acknowledge (ACK) 156 to commit the transaction if the result in the received tSP 154 is positive. Alternatively. the hand-held client can send the server a Cancel to abort the transaction. A typical example is that the client 140 requests to access information stored and identified by the URL as www.abc.com supported at the server 142, however, the URL in the tSR 152 is entered as www.abcd.com, the result in the tSP 154 returns a error message indicating the desired URL could not be found, otherwise the result in the tSP 154 shows the desired URL has been found, now it is up to the user of the client to determine if the client shall proceed with the tSP 156 or cancel to abort the current transaction to try a new or different URL.

[0050] Referring now to Figure 6, there is shown a schematic diagram of a notification transaction. A notification transaction can be initiated by either the client 140 or the server 142. In the case of server initiation, the server 142 initiates the notification transaction by sending to the client 140 a signal data unit, or notification request (NR) 162, to inform the client 140 that there is a notification in pending in the server 142, such as an electronic mail. waiting for immediate attentions from the identified client. Upon receiving of the NS 162, the client 140 sends a Get-Notify (ON) 164 to the server 142 and retrieves its notification contents such as alerts and emails. The server 142, as in the service transaction, replies with a tSR 146. The transaction is committed after an acknowledge signal (AS) 156 is sent to the server 142 and the server 142 receives it. In the case of the client notification, the client 140 initiates the notification transaction when it powers on or switches back to the

data mode from voice mode by asking the server 142 if there is any notification in pending. If there is notification in pending, the client 140 handles the notification transaction as if a signal is received. The AS 156 may be piggybacked with a GN when multiple notification transactions are conducted sequentially. If there are multiple notifications are pending at the server 142, the optional header in the tSR 146 indicates that so that the client will automatically start another notification transaction.

[0051] Referring now to Figure 7, there is shown the post transaction. Post transaction is initiated by the mobile client 140. The post transaction is used for a mobile device to update information stored in a WWW service as specified in the URL. The client 140 sends a Post Request (PR) 172, which contains a URL, data for updating, and an optional header. The server 142 processes the PR 172 and responds to the client with a tSR 146. The result in the tSR 146 comes from the WWW service and normally indicates if information update is done. Upon receiving of the tSR 146, the client 140 sends the server 142 an AS 156 to commit the transaction. Alternatively, the mobile client 140 can send the server 142 a Cancel to abort the transaction.

[0052] The present invention has been described in sufficient detail with one exemplary embodiment. Alternative embodiments will become apparent to those skilled in the art to which the present invention pertains. For example, wireless communications between a server and a personal digital assistant such as Palm Pilot from 3 Com Corporation and also a portable computer that runs under a operating system, for example, Windows CE from Microsoft Corporation. Accordingly, the scope of the present invention is defined by the appended claims rather than the forgoing description of one embodiment.

Claims

1. A method for establishing an authenticated and secure communication session for transactions between a client (106, 120, 140) and a server (114, 142) over a wireless data network (102), said client being remotely located with respect to said server, said method comprising:-

sending a session-request signal (SR, 144) from said client over said wireless data network to said server, said session-request signal including a client message, which is encrypted according to a shared secret encrypt key previously residing on both the client and the server;

conducting a first step of a client authentication at the server by checking for the successful decryption of the encrypted client message according to said shared secret encrypt key;

generating at the server a session key for said session, a first derivative of the decrypted client message, and a server message if the first step of the client authentication is successful;

sending a session-reply signal (SP, 146) from said server to said client over said wireless data network, said session-reply signal including said session key, said first derivative of the decrypted client message, and said server message, which are encrypted according to said shared secret encrypt key;

conducting a first step of a server authentication at said client by checking for the successful decryption of the encrypted session-reply signal according to said shared secret encrypt key, and retrieving said first derivative of the decrypted client message and said server message;

conducting a second step of the server authentication at said client by validating the first derivative of the client message with the client message included in the session-request signal;

generating at the client a first derivative of the decrypted server message if the server authentication is successful;

sending a session-complete signal (SC, 148) from said client to said server over said wireless data network, said session-complete signal including said first derivative of the decrypted server message, said first derivative being encrypted according to said shared secret encrypt key;

conducting a second step of the client authentication at said server by validating the first derivative of the decrypted server message with the server message included in the session-reply signal; and

establishing an authenticated and secure communication session if the second step of the client authentication is successful.

2. A method according to claim 1 wherein said session-request signal further includes a modified version of said client message, encrypted according to said shared secret encrypt key; wherein said modified version has an operational relationship with said client message.

3. A method according to claim 1 or 2 wherein said first derivative of the client message has a mathematical relationship with said client message.

4. A method according to any preceding claim wherein said client message comprises a client nonce.

5. A method according to any preceding claim wherein said first derivative of the server message has a mathematical relationship with said server mes-

sage.

6. A method according to any preceding claim wherein said server message comprises a server nonce.

7. A method according to any preceding claim wherein said session-complete signal is piggybacked by a transaction request from said client.

8. A method according to claim 7 wherein said transaction request is encrypted according to said session key included in the session-reply signal.

9. A method according to any preceding claim wherein said session-request signal further includes a device identifier associated with the client, and wherein the server determines said shared secret encrypt key based on the device identifier.

10. A method according to any preceding claim wherein the session-request signal includes a client cipher indicating what encryption the client currently uses.

11. A method according to claim 10 wherein the method further comprises the step of the server negotiating a mutually accepted cipher with the client for the session.

12. Apparatus for establishing an authenticated and secure communication session for transactions with a server (114, 142) over a wireless data network (102), said server being remotely located with respect to said apparatus, said apparatus comprising:-

a display screen (116);
memory for storing code for a client module (122);
a processor (610) coupled to said memory, said processor executing said code in said memory to cause said client module:-

to send a session-request signal (SR, 144) over said wireless data network to said server, said session-request signal including a client message, which is encrypted according to a shared secret encrypt key previously residing on both the apparatus and the server;
to conduct a first step of a server authentication by checking for the successful decryption of a session-reply signal (SP, 146), received from said server in response to said session-request signal, encrypted according to said shared secret encrypt key, and retrieving a first derivative of said client message and a server message;
to conduct a second step of the server authentication at said client by validating the decrypted first derivative of the client message with the client message included in the session-request signal;
to generate a first derivative of the decrypted server message if the server authentication is successful; and
to send a session-complete signal (SC, 148) to said server over said wireless data network, said session-complete signal including said first derivative of the decrypted server message, said first derivative being encrypted according to said shared secret encrypt key.

13. Apparatus according to claim 12 wherein said session-request signal further includes a modified version of said client message, encrypted according to said shared secret encrypt key; wherein said modified version has an operational relationship with said client message.

14. Apparatus according to claim 12 or 13 wherein said first derivative of the client message has a mathematical relationship with said client message.

15. Apparatus according to any one of claims 12 to 14 wherein said client message comprises a client nonce.

16. Apparatus according to any one of claims 12 to 15 wherein said processor causes said client module to piggyback a transaction request on said session-complete signal.

17. A method according to claim 16 wherein said processor causes said client module to encrypt said transaction request according to said session key included in the session-reply signal.

18. Apparatus according to any one of claims 12 to 17 wherein said session-request signal further includes an apparatus identifier so that the server can determine said shared secret encrypt key based on the apparatus identifier.

19. Apparatus according to any one of claims 12 to 17 wherein the session-request signal includes a client cipher indicating what encryption the apparatus currently uses.

Patentansprüche

1. Verfahren zum Aufbauen einer authentifizierten und sicheren Kommunikationssession für Transaktionen zwischen einem Klienten (106, 120, 140) und einem Server (114,142) über ein drahtloses Daten-

netzwerk (102), wobei der Klient in Bezug auf den Server entfernt angeordnet ist, wobei das Verfahren folgendes aufweist:

Senden eines Session-Anforderungssignals (SR, 144) vom Klienten über das drahtlose Datennetzwerk zum Server, wobei das Session-Anforderungssignal eine Klientennachricht enthält, die gemäß einem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist, der zuvor auf sowohl dem Klienten als auch dem Server liegt;

Durchführen eines ersten Schritts einer Klientenauthentifizierung beim Server durch Prüfen auf die erfolgreiche Entschlüsselung der verschlüsselten Klientennachricht gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel;

Erzeugen eines Sessionschlüssels für die Session, einer ersten Ableitung der entschlüsselten Klientennachricht und einer Servemachricht beim Server, wenn der erste Schritt der Klientenauthentifizierung erfolgreich ist;

Senden eines Session-Antwortsignals (SP, 146) vom Server zum Klienten über das drahtlose Datennetzwerk, wobei das Session-Antwortsignal den Sessionschlüssel, die erste Ableitung der entschlüsselten Klientennachricht und die Servemachricht enthält, die gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt sind;

Durchführen eines ersten Schritts einer Serverauthentifizierung beim Klienten durch Prüfen auf die erfolgreiche Entschlüsselung des verschlüsselten Session-Antwortsignals gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel und Wiedergewinnen der ersten Ableitung der entschlüsselten Klientennachricht und der Servemachricht;

Durchführen eines zweiten Schritts der Serverauthentifizierung beim Klienten durch für gültig Erklären der ersten Ableitung der Klientennachricht mit der im Session-Anforderungssignal enthaltenen Klientennachricht;

Erzeugen einer ersten Ableitung der entschlüsselten Servemachricht beim Klienten, wenn die Serverauthentifizierung erfolgreich ist;

Senden eines Session-Beendigungssignals (SC, 148) vom Klienten über das drahtlose Datennetzwerk zum Server, wobei das Session-Beendigungssignal die erste Ableitung der entschlüsselten Servemachricht enthält, wobei die erste Ableitung gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist;

Durchführen eines zweiten Schritts der Klientenauthentifizierung beim Server durch für gültig Erklären der ersten Ableitung der entschlüsselten Servemachricht mit der im Session-Antwortsignal enthaltenen Servemachricht; und

Aufbauen einer authentifizierten und sicheren Kommunikationssession, wenn der zweite Schritte der Klientenauthentifizierung erfolgreich ist.

2. Verfahren nach Anspruch 1, wobei das Session-Anforderungssignal weiterhin eine modifizierte Version der Klientennachricht enthält, die gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist; wobei die modifizierte Version eine betriebsmäßige Beziehung zur Klientennachricht hat.

3. Verfahren nach Anspruch 1 oder 2, wobei die erste Ableitung der Klientennachricht eine mathematische Beziehung zur Klientennachricht hat.

4. Verfahren nach einem der vorangehenden Ansprüche, wobei die Klientennachricht eine Klienten-ad-hoc-Bildung aufweist.

5. Verfahren nach einem der vorangehenden Ansprüche, wobei die erste Ableitung der Servemachricht eine mathematische Beziehung zur Servernachricht hat.

6. Verfahren nach einem der vorangehenden Ansprüche, wobei die Servernachricht eine Server-ad-hoc-Bildung aufweist.

7. Verfahren nach einem der vorangehenden Ansprüche, wobei das Session-Beendigungssignal durch eine Transaktionsanforderung vom Klienten im Huckepack getragen wind.

8. Verfahren nach Anspruch 7, wobei die Transaktionsanforderung gemäß dem im Session-Antwortsignal enthaltenen Sessionschlüssel verschlüsselt wird.

9. Verfahren nach einem der vorangehenden Ansprüche, wobei das Session-Anforderungssignal weiterhin einen Vorrichtungsidentifizierer enthält, der zum Klienten gehört, und wobei der Server den gemeinsam genutzten geheimen Verschlüsselungsschlüssel basierend auf dem Vorrichtungsidentifizierer bestimmt.

10. Verfahren nach einem der vorangehenden Ansprüche, wobei das Session-Anforderungssignal einen Klientenschlüssel enthält, der anzeigt, welche Verschlüsselung der Klient gerade verwendet.

11. Verfahren nach Anspruch 10, wobei das Verfahren weiterhin den Schritt der Serververhandlung eines wechselseitig akzeptierten Schlüssels mit dem

Klienten für die Session aufweist.

12. Vorrichtung zum Aufbauen einer authentifizierten und sicheren Kommunikationssession für Transaktionen mit einem Server (114, 142) über ein drahtloses Datennetzwerk (102), wobei der Server in Bezug auf die Vorrichtung entfernt angeordnet ist, wobei die Vorrichtung folgendes aufweist:

einen Anzeigeschirm (116);
einen Speicher zum Speichern eines Codes für ein Klientenmodul (122);
einen Prozessor (610), der mit dem Speicher gekoppelt ist, wobei der Prozessor den Code im Speicher ausführt, um das Klientenmodul zu Folgendem zu veranlassen:

ein Session-Anforderungssignal (SR, 144) über das drahtlose Datennetzwerk zum Server zu senden, wobei das Session-Anforderungssignal eine Klientennachricht enthalt, die gemäß einem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist, der zuvor auf sowohl der Vorrichtung als auch dem Server liegt;
einen ersten Schritt einer Serverauthentifizierung durch Prüfen auf die erfolgreiche Entschlüsselung eines Session-Antwortsignals (SP, 146) durchzuführen, das vom Server in Reaktion auf das Session-Anforderungssignal empfangen wird, das gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist, und eine erste Ableitung der Klientennachricht und einer Servemachricht wiederzugewinnen;
einen zweiten Schritt der Serverauthentifizierung beim Klienten durch für gültig Erklären der entschlüsselten ersten Ableitung der
Klientennachricht mit der im Session-Anforderungssignal enthaltenen Klientennachricht durchzuführen;
eine erste Ableitung der entschlüsselten Servemachricht zu erzeugen, wenn die Serverauthentifizierung erfolgreich ist; und ein Session-Beendigungssignal (SC, 148) über das drahtlose Datennetzwerk zum Server zu senden; wobei das Session-Beendigungssignal die erste Ableitung der entschlüsselten Servemachricht enthält, wobei die erste Ableitung gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist.

13. Vorrichtung nach Anspruch 12, wobei das Session-Anforderungssignal weiterhin eine modifizierte Version der Klientennachricht enthält, die gemäß dem gemeinsam genutzten geheimen Verschlüsselungsschlüssel verschlüsselt ist; wobei die modifizierte Version eine betriebsmäßige Beziehung zur Klientennachricht hat.

14. Vorrichtung nach Anspruch 12 oder 13, wobei die erste Ableitung der Klientennachricht eine mathematische Beziehung zur Klientennachricht hat.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, wobei die Klientennachricht eine Klienten-ad-hoc-Bildung aufweist.

16. Vorrichtung nach einem der Ansprüche 12 bis 15; wobei der Prozessor veranlasst, dass das Klientenmodul eine Transaktionsanforderung auf dem Session-Beendigungssignal im Huckepack trägt.

17. Verfahren nach Anspruch 16, wobei der Prozessor veranlasst, dass das Klientenmodul die Transaktionsanforderung gemäß dem im Session-Antwortsignal enthaltenen Sessionschlüssel verschlüsselt.

18. Vorrichtung nach einem der Ansprüche 12 bis 17, wobei das Session-Anforderungssignal weiterhin einen Vorrichtungsidentifizierer enthält, so dass der Server den gemeinsam genutzten geheimen Verschlüsselungsschlüssel basierend auf dem Vorrichtungsidentifizierer bestimmen kann.

19. Vorrichtung nach einem der Ansprüche 12 bis 17, wobei das Session-Anforderungssignal einen Klientenschlüssel enthält, der anzeigt, weiche Verschlüsselung die Vorrichtung gerade verwendet.

Revendications

1. procédé pour établir une session de communication authentifiée et sécurisée pour des transactions entre un client (106, 120, 140) et un serveur (114, 142) sur un réseau de données sans fil (102), ledit client étant situé à distance par rapport audit serveur, ledit procédé comprenant les opérations consistant à :

- envoyer un signal de requête de cession (SR, 144), sur ledit réseau de données sans fil, dudit client audit serveur, ledit signal de requête de session comprenant un message de client, qui est :crypté conformément à une clé de cryptage secrète partagée, résidant préalablement à la fois sur le client et sur le serveur ;
- conduire une première étape d'une authentification de client au niveau du serveur en contrôlant le décryptage réussi du message de client crypté conformément à ladite clé de cryptage secrète partagée ;

- générer au niveau du serveur une clé de session pour ladite session, un premier dérivé du message de client décrypté et un message de serveur si la première étape de l'authentification de client est réussie ;
- envoyer un signal de réponse de session (SP, 146) dudit serveur audit client sur ledit réseau de données sans fil, ledit signal de réponse de session: incluant ladite clé de session, ledit premier dérivé du message de client décrypté et ledit message de serveur, qui sont cryptés conformément à ladite clé de cryptage secrète partagée ;
- conduire une première étape d'une authentification de serveur au niveau dudit client en contrôlant le décryptage réussi du signal de réponse de session crypté conformément à ladite clé de cryptage secrète partagée, et récupérer ledit premier dérivé du message de client décrypté: et ledit message de serveur ;
- conduire une deuxième étape de l'authentification de serveur au niveau dudit client en validant le premier dérivé du message de client avec le message de client inclus dans le signal de requête de session ;
- générer, au niveau du client, un premier dérivé du message de serveur décrypté si l'authentification du serveur est réussie ;
- envoyer un signal d'achèvement de session (SC, 148) dudit client audit serveur sur ledit réseau de données sans fil, ledit signal d'achèvement de! session incluant ledit premier dérivé du message de serveur décrypté, ledit premier dérivé étant crypté conformément à ladite clé de cryptage secrète partagée ;
- conduire une deuxième étape de l'authentification de client au niveau dudit serveur en validant le premier dérivé du message de serveur décrypté avec le message de serveur inclus dans le signal de réponse de session ; et
- établir une session de communication authentifiée et sécurisée si la deuxième étape de l'authentification de client est réussie.

2. Procédé selon la revendication 1, dans lequel ledit signal de requête de session inclut en outre une version modifiée dudit message : de client, cryptée conformément à ladite clé de cryptage secrète partagée ; dans lequel ladite version modifiée a une relation opérationnelle avec ledit message de client.

3. Procédé selon l'une des revendications 1 ou 2, dans lequel ledit premier dérivé du message de client a une relation mathématique avec ledit message de client.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit message de client comprend un nonce de client.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit premier dérivé du: message de serveur a une relation mathématique avec ledit message de serveur.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit message de serveur comprend un nonce de serveur.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel une requête de transaction dudit client est superposée audit signal d'achèvement de session.

8. Procédé selon la revendication 7, dans lequel ladite requête de transaction est cryptée conformément à ladite clé de session incluse: dans le signal de réponse de session.

9. Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit signal de requête de session inclut en outre un identificateur de dispositif associé au.client, et dans lequel le serveur détermine ladite clé de cryptage secrète partagée sur la base de l'identificateur de dispositif.

10. Procédé selon l'une quelconque des revendications précédentes, dans lequel le signal de requête de session inclut un chiffre de client indiquant quel cryptage le client utilise de façon courante.

11. Procédé selon la revendication 10, dans lequel le procédé comprend en outre l'étape de négociation par le serveur, avec le client, d'un chiffre mutuellement accepté pour la session.

12. Appareil pour établir une session de communication authentifiée et sécurisée pour des transactions avec un serveur (114, 142) sur un réseau de données sans fil (102), ledit serveur étant situé à distance par rapport: audit appareil, ledit :appareil comprenant :

- un écran d'affichage (116) ;
- une mémoire pour mémoriser un code pour un module de client (122) ;
- un processeur (610) couplé à ladite mémoire, ledit processeur exécutant ledit code dans ladite mémoire pour amener ledit module de client à :

  - envoyer audit serveur un signal de requête de session (SR, 144) sur ledit réseau de données sans fil, ladite requête de demande de session: incluant un message de

client, qui est crypté conformément à une clé de cryptage secrète partagée, résidant préalablement à la fois sur l'appareil et sur le serveur ;

- conduire une première étape d'une authentification de serveur en contrôlant le décryptage réussi d'un signal de réponse de session (SP, 146), reçu dudit serveur en réponse audit signal de requête de session, crypté conformément à ladite clé de cryptage secrète partagée, et récupérer un premier dérivé dudit message de client et un message de serveur ;
- conduire, au niveau dudit :client, une : deuxième étape de l'authentification:de serveur en validant le premier dérivé décrypté du message de client avec le message de client inclus dans le signal de requête de session ;
- générer un premier dérivé du message de serveur décrypté si l'authentification de serveur est réussie ; et
- envoyer un signal d'achèvement de session (SC, 148) audit serveur sur ledit réseau de données sans fil, ledit signal d'achèvement de session incluant ledit premier dérivé du message de serveur décrypté, ledit premier dérivé étant crypté conformément à ladite clé de :cryptage secrète partagée.

13. Appareil selon la revendication 12, dans lequel ledit signal de requête de session inclut en outre une version modifiée dudit message de client, cryptée conformément à ladite clé de cryptage secrète partagée ; dans lequel ladite version modifiée a une relation opérationnelle avec ledit message de client.

14. Appareil selon l'une des revendications 12 ou 13, dans lequel ledit premier :dérivé du message de client a une relation mathématique avec ledit message de client.

15. Appareil selon l'une quelconque des revendications 12 à 14, dans lequel ledit message de client comprend un nonce de client.

16. Appareil selon l'une quelconque des revendications 12 à 15, dans lequel:ledit processeur amène ledit module de client à superposer une requête de transaction sur ledit signal d'achèvement de session.

17. Appareil selon la revendication :16, dans lequel ledit processeur amène ledit module de client à crypter ladite requête de transaction conformément à ladite clé de session incluse dans le signal de réponse de session.

18. Appareil selon l'une quelconque des revendications 12 à 17, dans lequel ledit signal de demande de session inclut en outre un identificateur d'appareil de telle sorte que le serveur puisse déterminer ladite clé de cryptage secrète partagée sur la base de l'identifücateur d'appareil.

19. Appareil selon l'une quelconque des revendications 12 à 17, dans lequel le signal de requête de session comprend un chiffre de client indiquant quel cryptage l'appareil utilise de façon courante.

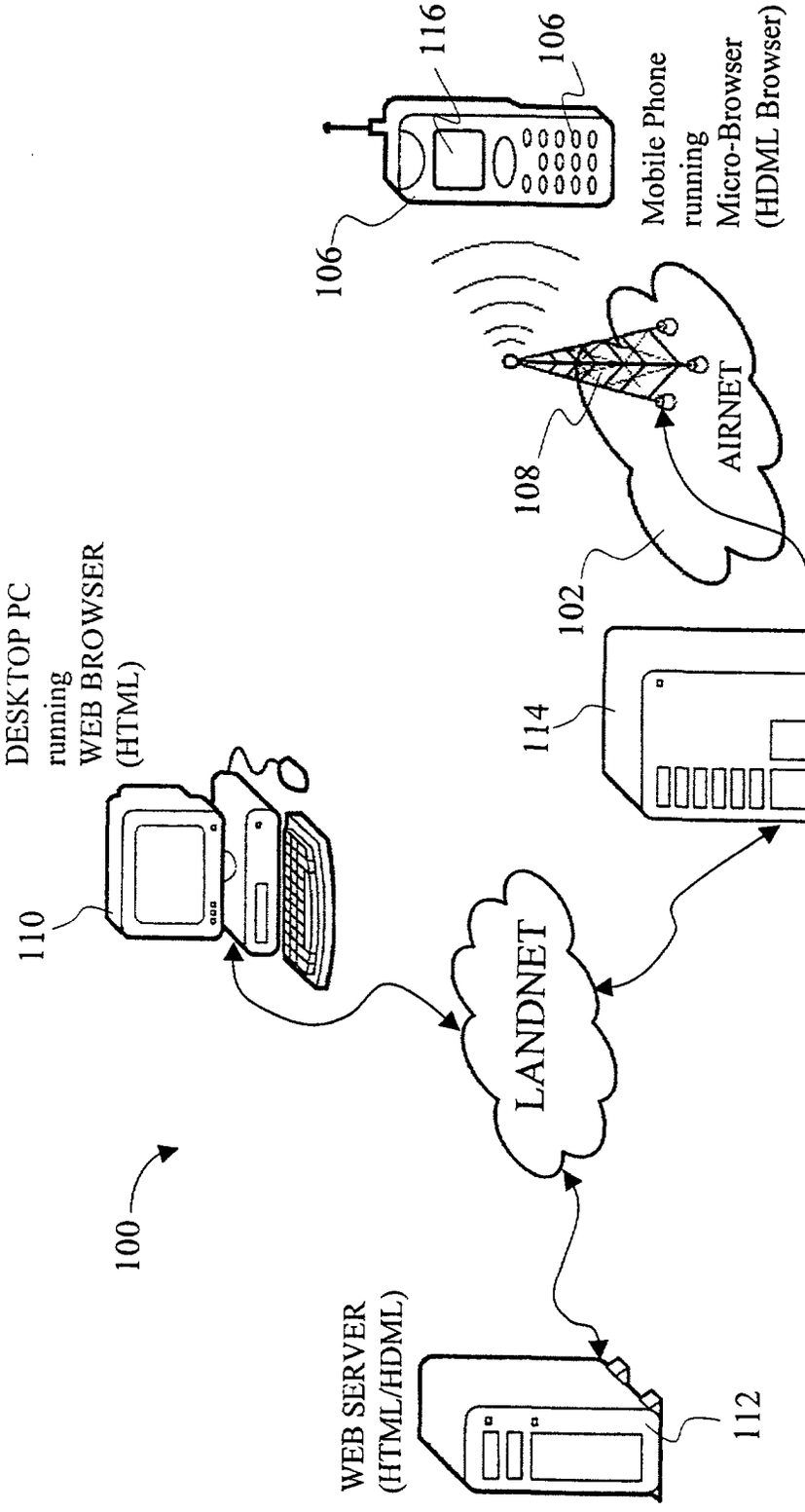

100
110
DESKTOP PC
running
WEB BROWSER
(HTML)
LANDNET
WEB SERVER
(HTML/HDML)
112
114
UP.LINK
GATEWAY
(HTTP<-->HDTP)
102
AIRNET
108
106
116
106
Mobile Phone
running
Micro-Browser
(HDML Browser)

Fig. 1

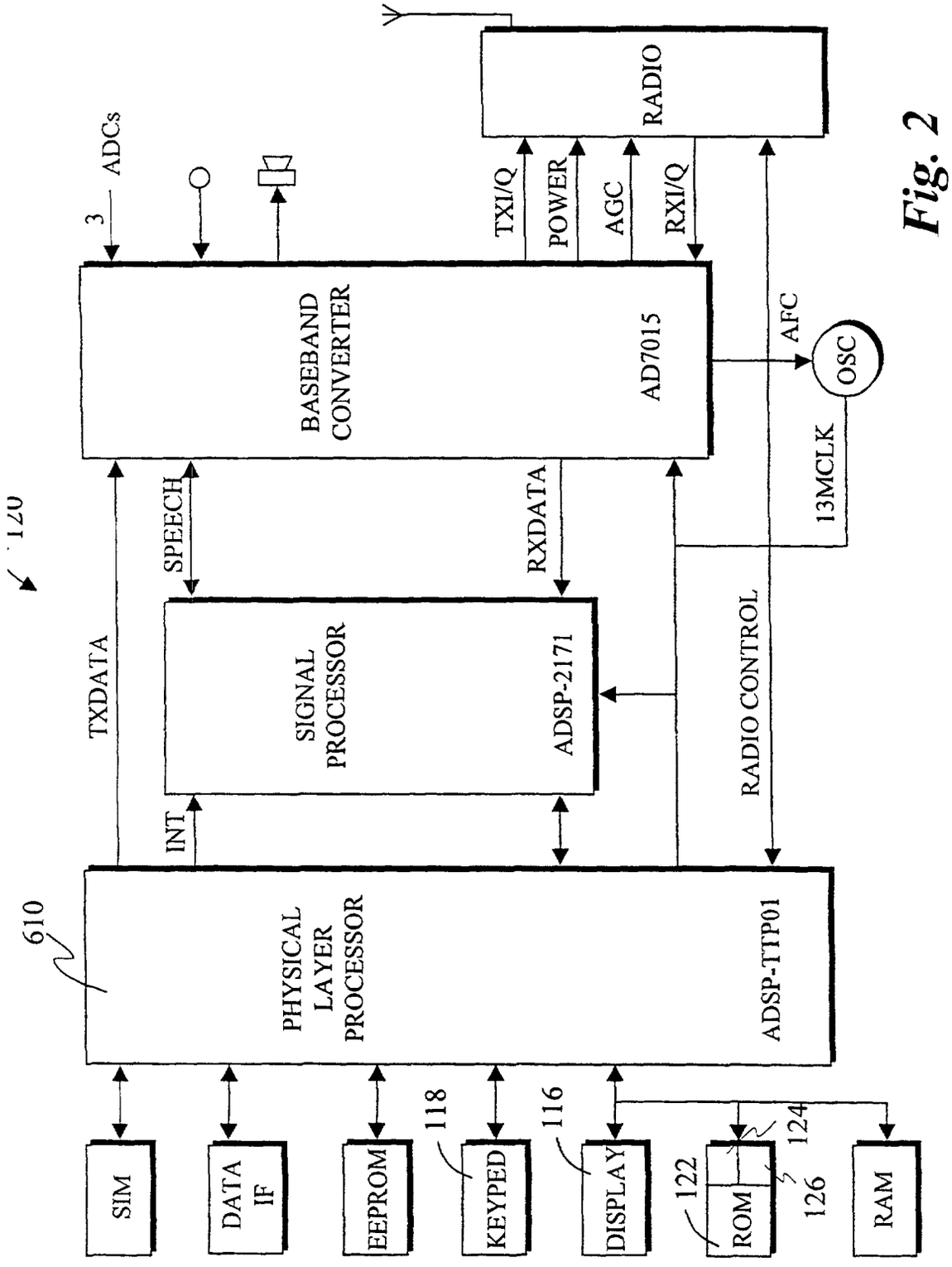

120
610
PHYSICAL LAYER PROCESSOR
ADSP-TTP01
SIGNAL PROCESSOR
ADSP-2171
BASEBAND CONVERTER
AD7015
RADIO
ADCs
3
TXDATA
SPEECH
INT
RXDATA
RADIO CONTROL
TXI/Q
POWER
AGC
RXI/Q
AFC
OSC
13MCLK
SIM
DATA IF
EEPROM
KEYPED
DISPLAY
ROM
RAM
118
116
122
124
126

Fig. 2

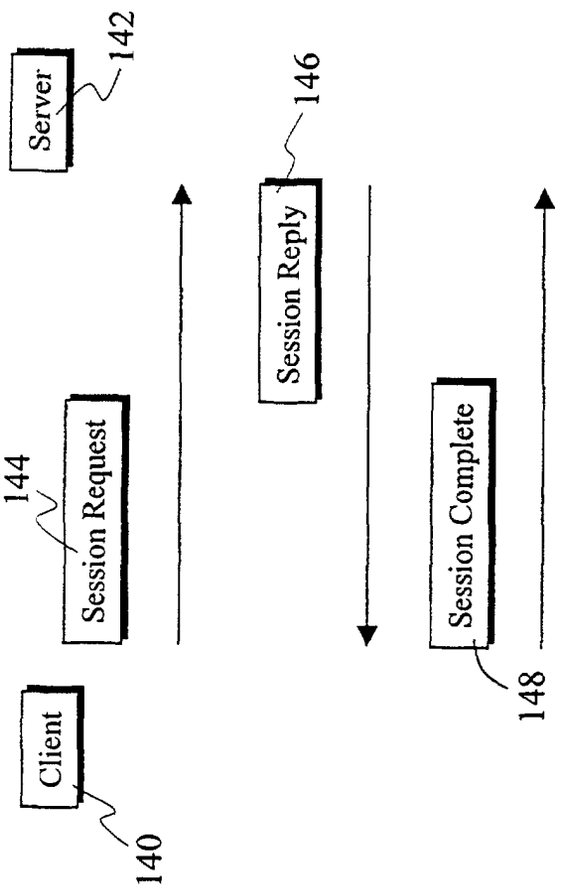
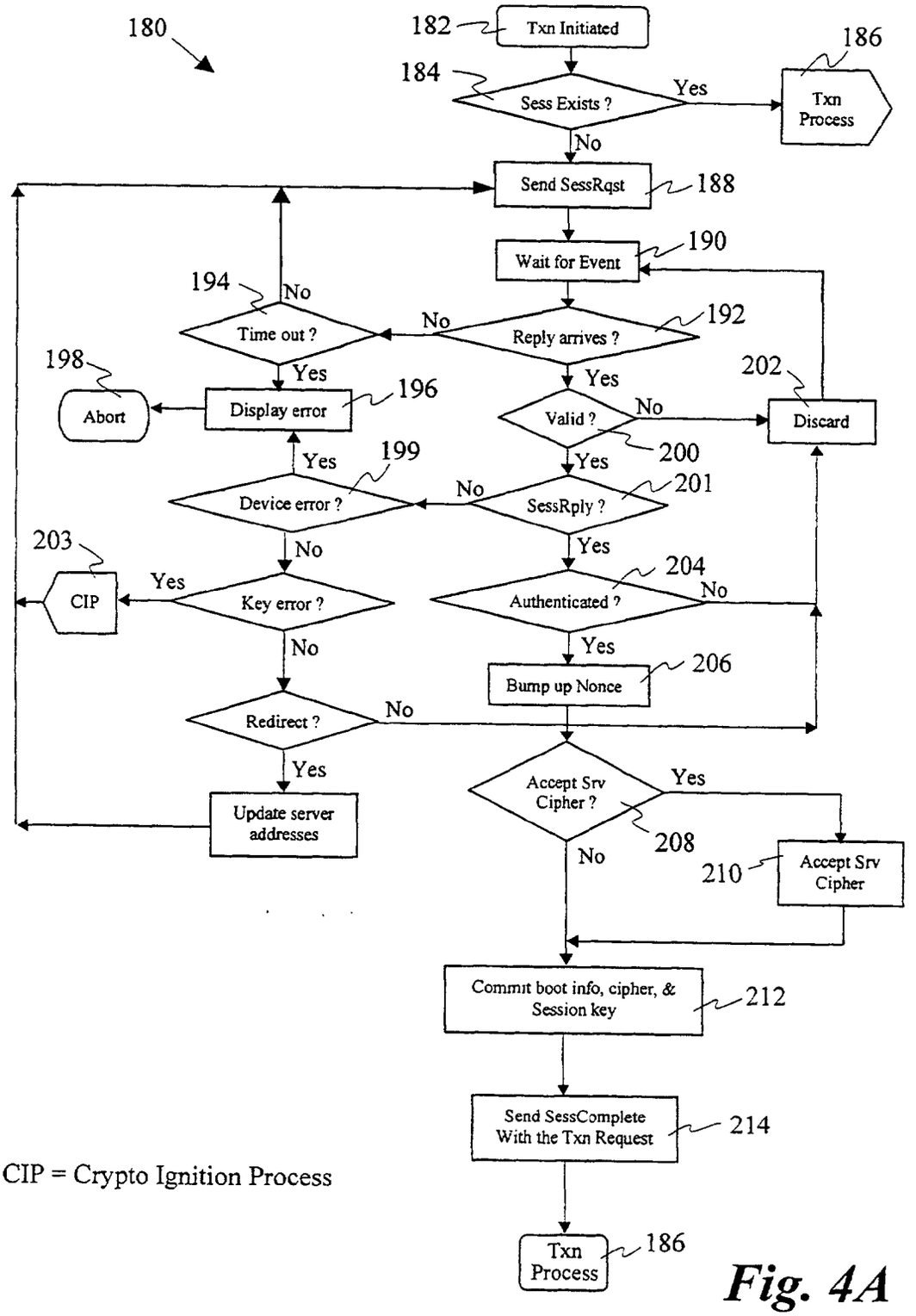
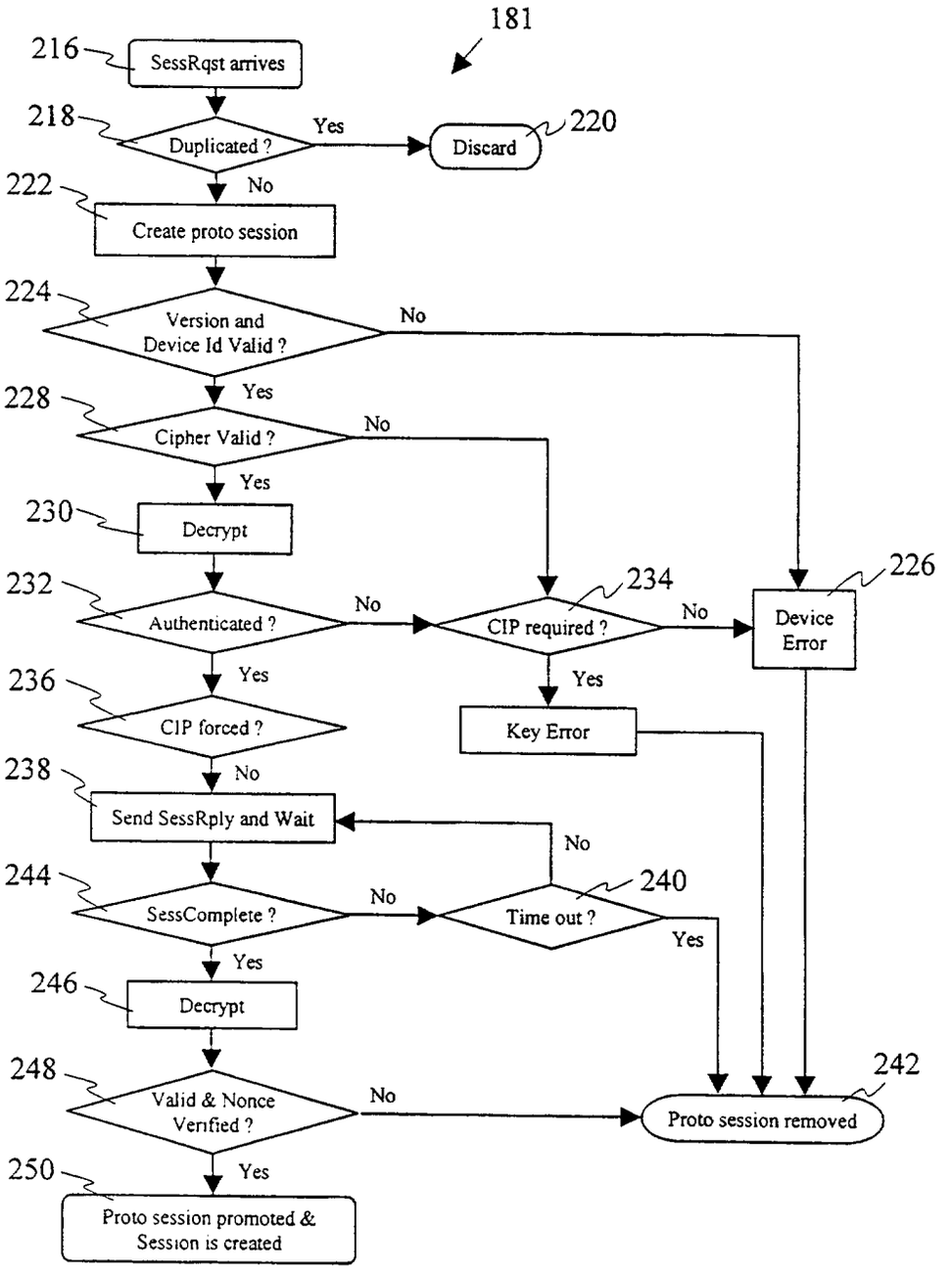

Server
142
146
Session Reply
144
Session Request
Session Complete
Client
140
148

Fig. 3



CIP = Crypto Ignition Process

Fig. 4A



CIP = Crypto Ignition Process

Fig. 4B

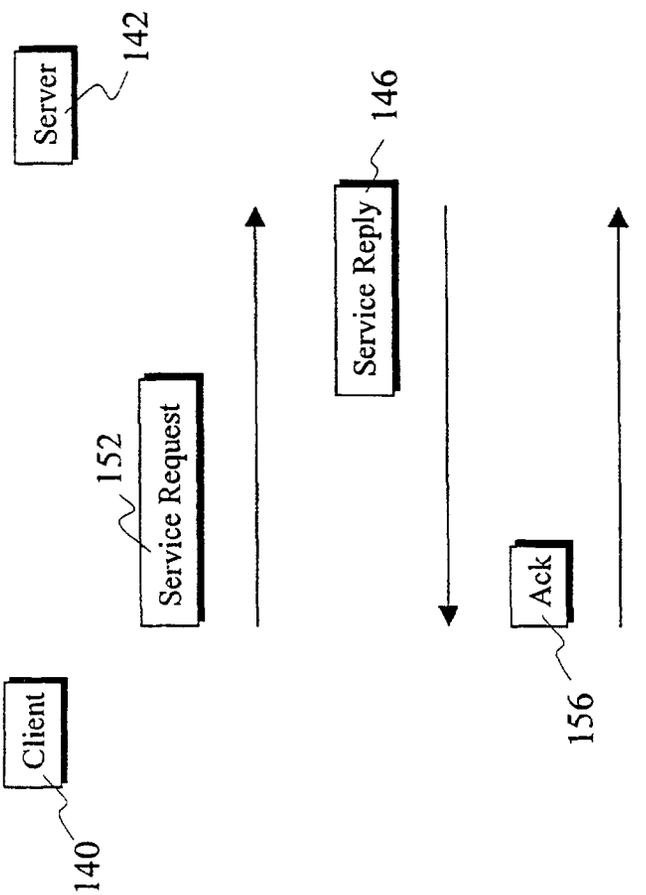

Client
140
Server
142
Service Request
152
Service Reply
146
Ack
156

Fig. 5

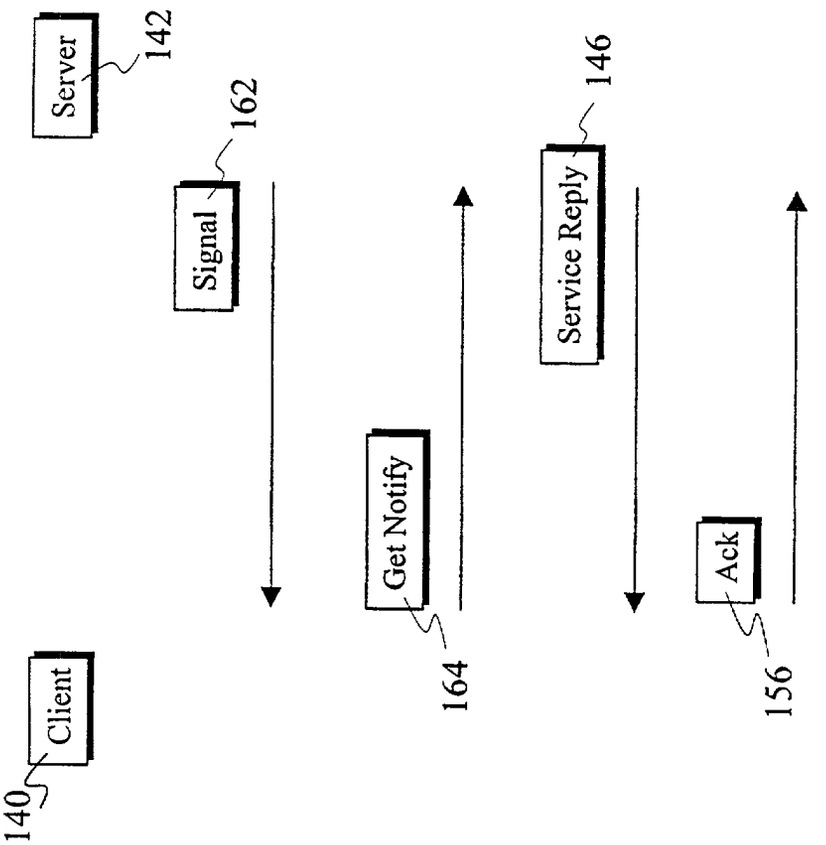

Client
140
Server
142
Signal
162
Get Notify
164
Service Reply
146
Ack
156

Fig. 6

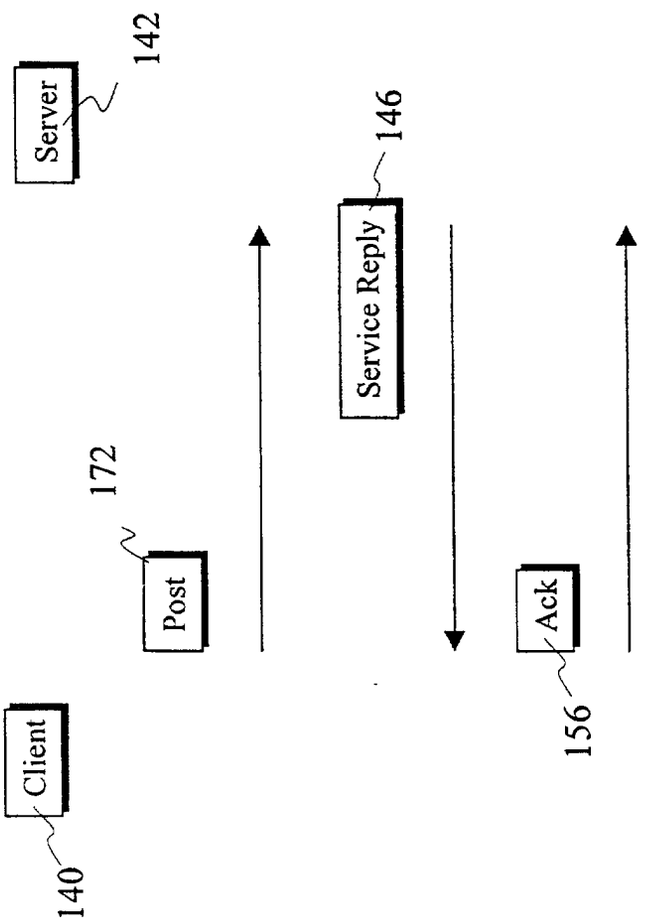


Fig. 7